ABSTRACT OF THE DISCLOSURE

SYSTEM, METHOD, AND PROGRAM FOR MANAGING A USER KEY USED TO SIGN A MESSAGE FOR A DATA PROCESSING SYSTEM

A system, method, and program for managing a user key used to sign a message for a data processing system having an encryption chip are disclosed. A user is assigned a user key. In order to encrypt and send messages to a recipient(s), the messages are encrypted with the user key. The user key, in turn, is encrypted with an associated key. The associated key is further encrypted using an encryption chip key stored on the encryption chip. The encrypted messages are communicated to a recipient to validate an association of the user with the encrypted messages. The associated key is decrypted with the encryption chip key. The user key is decrypted with the associated key, and the messages are decrypted with the user key. Thereafter, validation of the association of messages with the user is removed by revoking the associated key. In a preferred embodiment, encryption resources are centralized in a server system having the encryption chip. The server system is coupled to and provides encryption services to a plurality of client systems. Messages to be encrypted are sent from a user's client system to the server system, which encrypts the messages using the encryption chip. The encrypted messages are sent from the server system to the client system, which then transmits the encrypted messages to their intended recipient(s). All data relating to the encrypted messages are erased from the server system after the encrypted messages are sent from the server system to the client system.